UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,957	09/03/2004	Alexander Shipp	SYMC1198	1437

34350 7590 07/31/2009

GUNNISON, MCKAY & HODGSON, L.L.P.
1900 GARDEN ROAD, SUITE 220
MONTEREY, CA 93940

EXAMINER	
PHAM, MICHAEL	
ART UNIT	PAPER NUMBER
2167	
MAIL DATE	DELIVERY MODE
07/31/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/500,957	SHIPP, ALEXANDER	
	Examiner	Art Unit	
	MICHAEL PHAM	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-7 and 9-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-7 and 9-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Status

1. Claims 1, 3-7, and 9-13 are pending and have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1, 7, and 13 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant's state that "a factor that the longer the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected the more likely the file is safe" is supported on page 3 lines 1-12. However, this is either unclear as written or is clearly not supported since on page 3 lines 9-12 states that "The longer the time that passes, the more likely it is that a suspicious person will submit a file containing malware to the developers of the scanner, who will analy[z]e the file, and update their scanner to detect it" In other words, as time increases the more likely the file is not safe because a suspicious person is more likely to submit a file containing malware.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1 and 3-6 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

MPEP 2106:

The claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 U.S.C. 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best functional descriptive material per se.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material". Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare In re Lowry, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994)

Merely claiming nonfunctional descriptive material, i.e. abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See Diehr, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in Benson were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer"

Claim 1 recites "a system". However, claim 1 fails to contain any computer hardware that is used to implement the system so as to realize its functionality. Thus, the body of claim 1 is merely an abstract idea and is being processed without any computer hardware manipulation. Contrary to arguments made by some Applicants, use of the word "system" does not inherently mean that the claim is directed to a machine. Only if at least one of the claimed elements of the

system is a physical part of a device can the system as claimed constitute part of a device or a combination of devices to be a machine within the meaning of 101. In regards to "computer apparatus", this does not necessitate hardware, and is neither an element of the system. In regards to figure 1, figure 1 discloses a block diagram of a method, it does not necessitate hardware for the system. Claims 3-6 fail to resolve the deficiencies of claim 1 and are therefore rejected.

6. Claim 13 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

MPEP 2106:

The claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 U.S.C. 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best functional descriptive material per se.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material". Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare In re Lowry, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994)

Merely claiming nonfunctional descriptive material, i.e. abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See Diehr, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in Benson were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer"

Claim 13 recites "a system". However, claim 1 fails to contain any computer hardware that is used to implement the system so as to realize its functionality. Thus, the body of claim 13

is merely an abstract idea and is being processed without any computer hardware manipulation. Contrary to arguments made by some Applicants, use of the word "system" does not inherently mean that the claim is directed to a machine. Only if at least one of the claimed elements of the system is a physical part of a device can the system as claimed constitute part of a device or a combination of devices to be a machine within the meaning of 101. In regards to "computer apparatus", this does not necessitate hardware, and is neither an element of the system. In regards to figure 1, figure 1 discloses a block diagram of a method, it does not necessitate hardware for the system.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 3-7, 9-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication Number 2004/0088570 issued to Guy William Welch Roberts et al (hereafter Roberts) in view of US Patent 6721721 by Bates et. al. (hereafter Bates).

Claim 1:

Roberts discloses the following claimed limitations:

"a) means for generating data with regard to the file to characterize its identity and for thereby referencing a computer database to determine whether it is an instance of a known file" [0033 lines 8-12, removing the internet address from the currently held data (e.g. stripping the internet address from the e-mail or the data file and possibly replacing it with a marker indicating that it has been removed because it pointed to malware.). 0034, store data identifying malware free content that may be accessed over the internet. This may take the form of a database storing internet addresses that have been pre-emptively scanned for malware content in accordance with the previous steps and found not to contain malware (together with page version identifying data such as date, filesize, checksum, etc). Accordingly, means for generating data (marker) with regard to the file (data) to characterize its identity (pointed to malware) and for thereby referencing a computer database (database) to determine whether it is an instance of a known file (identifying malware free content)]

"b) means for selectively subjecting the file to a number of heuristic procedures to determine whether or not it contains, or is likely to contain, malware" [0037-0038, and Figure 6, elements 42-48. Accordingly, b) means for selectively subjecting the file to a number of heuristic procedures (figure 6 elements 42-48) to determine whether or not it contains, or is likely to contain, malware (figure 6 element 46)]

"c) means for determining, in dependence upon the record, if any, of the file in the database, whether the file can be regarded as safe in dependence on factors"[0034, lines 1-7, store data identifying malware free content that may be accessed over the internet. This may take the form

of a database storing internet addresses that have been pre-emptively scanned for malware content in accordance with the previous steps and found not to contain malware (together with page version identifying data such as date, filesize, checksum, etc). figure 6. Accordingly, c) means for determining (figure 6), in dependence upon the record (database), if any, of the file in the database (database storing internet addresses that have been pre-emptively scanned), whether the file can be regarded as safe (identifying malware free content, figure 6 step 50) in dependence on factors (date, filesize, checksum)]

"and for controlling the means b) such that the file, if the file is to be regarded as safe, is either subject to less thorough processing than if it were not so regarded or not subject to processing by the means b) at all" [0034, lines 1-7, store data identifying malware free content that may be accessed over the internet. This may take the form of a database storing internet addresses that have been pre-emptively scanned for malware content in accordance with the previous steps and found not to contain malware (together with page version identifying data such as date, filesize, checksum, etc). 0037 lines 12-16, if the checksums match then the webpage may be assumed to not have been changed in the intervening period and not require rescanning for malware prior to being returned to the requester. Accordingly, and for controlling the means b) such that the file (data/webpage/content), if the file is to be regarded as safe (malware free content), is either subject to less thorough processing than if it were not so regarded or not subject to processing by the means b) at all (not require rescanning) is disclosed].

Roberts does not explicitly teach factors including the "a factor that the longer length of time which the database indicates that the file has been known without malware-containing instances of it being detected the more likely that the file is safe."

On the other hand, Bates discloses if the URL was not found to be untrustworthy, control passes to block 98 to determine whether a "good" url threshold time has past-that is, whether an excessive period of time has elapsed since the URL was last virus checked. Figure 3 elements 96-99. Accordingly, a factor that the longer the length of time (threshold time passed) which the database indicates that the file has been known without malware containing instances of it being detected (no virus in the past)the more likely that the file is safe (checked) .

Both Roberts and Bates are directed to the same field of endeavor as applicant's invention. Both are directed to improving virus scanning systems. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have applied the disclosure of Bates above to the disclosure of Roberts for the purpose of reducing the time of scanning for a virus, and to ensure that virus status information for URL's in the virus database is kept relatively current (Bates, col. 14 lines 1-5).

Claims 3 and 9:

As per claims 3 and similarly claim 9, the combination of Roberts and Bates disclose in Roberts: "wherein the means c) performs said determining of whether a file can be regarded as safe in

dependence on factors including sources, recorded in the database, from which instances of the file have originated"[paragraph 34, lines 1-6, Internet address]

Claims 4 and 10:

As per claims 4 and similarly claim 10, the combination of Roberts and Bates disclose in Roberts: "performs said determining of whether a file can be regarded as safe in dependence on factors including the number of times, recorded in the database, instances of the file have been processed" [paragraph 37, lines 8-18, checksum comparison and a mechanism which uses dates and other information to determine currency and status]

Claims 5 and 11:

As per claims 5 and similarly claim 11, the combination of Roberts and Bates disclose in Roberts: "means for updating the database in dependence upon the result of the processing of the file by the means b)" [paragraph 33, virus found actions include updating]

Claims 6 and 12:

As per claims 5 and similarly claim 11, the combination of Roberts and Bates disclose in Roberts: "wherein the updating of the database, is operative in the event of the means b) determining that the file contains, or is likely to contain, malware to delete the record of the file in the database or to update the record of the file in the database so that the file no longer is taken be safe" [paragraph 33, virus found actions].

Claim 7:

As per claim 7, similar as claim 1 above and Roberts further teaches storing the determination of whether or not the file contains, or is likely to contain malware [0034, lines 1-7, store data identifying malware free content that may be accessed over the internet. This may take the form of a database storing internet addresses that have been pre-emptively scanned for malware content in accordance with the previous steps and found not to contain malware (together with page version identifying data such as date, filesize, checksum, etc.) Accordingly, disclosing storing the determination of whether or not the file contains or is likely to contain malware (store data identifying malware free content)]

Claim 13

As per claim 13 Roberts discloses the following claimed limitations:
"an engine that generates data with regard to the file to characterize its identity and for thereby referencing a computer database to determine whether it is an instance of a known file" [0033 lines 8-12, removing the internet address from the currently held data (e.g. stripping the internet address from the e-mail or the data file and possibly replacing it with a marker indicating that it has been removed because it pointed to malware.). 0034, store data identifying malware free content that may be accessed over the internet. This may take the form of a database storing internet addresses that have been pre-emptively scanned for malware content in accordance with the previous steps and found not to contain malware (together with page version identifying data such as date, filesize, checksum, etc). Accordingly, an engine (step 30) that generates data (marker) with regard to the file (data) to characterize its identity (pointed to malware) and for

thereby referencing a computer database (database) to determine whether it is an instance of a known file (identifying malware free content)]

"that processes the file by selectively subjecting the file to a number of heuristic procedures to determine whether or not it contains, or is likely to contain, malware" [0037-0038, and Figure 6, elements 42-48. Accordingly, that processes the file by selectively subjecting the file to a number of heuristic procedures (figure 6 elements 42-48) to determine whether or not it contains, or is likely to contain, malware (figure 6 element 46)]

"and that determines, in dependence upon the record, if any, of the file in the database, whether the file can be regarded as safe in dependence on factors including the length of time for which the database indicates that the file has been known without malware- containing instances of it being detected" [0034, lines 1-7, store data identifying malware free content that may be accessed over the internet. This may take the form of a database storing internet addresses that have been pre-emptively scanned for malware content in accordance with the previous steps and found not to contain malware (together with page version identifying data such as date, filesize, checksum, etc). figure 6. Accordingly, and that determines, in dependence upon the record (database), if any, of the file in the database (database storing internet addresses that have been pre-emptively scanned. 0034, lines 8-10, data referred to by the internet addresses may also be stored), whether the file can be regarded as safe (identifying malware free content, figure 6 step 50) in dependence on factors (date, filesize, checksum)]

"and controls the processing to which the file is subjected such that the file, if the file is to be regarded as safe, is either subject to less thorough processing than if it were not so regarded or not subject to the processing at all" [0034, lines 1-7, store data identifying malware free content that may be accessed over the internet. This may take the form of a database storing internet addresses that have been pre-emptively scanned for malware content in accordance with the previous steps and found not to contain malware (together with page version identifying data such as date, filesize, checksum, etc). 0037 lines 12-16, if the checksums match then the webpage may be assumed to not have been changed in the intervening period and not reuire rescanning for malware prior to being returned to the requester. Accordingly, and for controlling the processing to which the file is subjected such that the file (data/webpage/content), if the file is to be regarded as safe (malware free content), is either subject to less thorough processing than if it were not so regarded or not subject to processing at all (not require rescanning) is disclosed].

Roberts does not explicitly disclose dependence on factors including the "a factor that the longer the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected the more likely that the file is safe"

On the other hand, Bates discloses if the URL was not found to be untrustworthy, control passes to block 98 to determine whether a "good" url threshold time has past-that is, whether an excessive period of time has elapsed since the URL was last virus checked. Figure 3 elements 96-99. Accordingly, a factor that the longer the length of time (threshold time passed) which the

database indicates that the file has been known without malware containing instances of it being detected (no virus in the past)the more likely that the file is safe (checked) .

Both Roberts and Bates are directed to the same field of endeavor as applicant's invention. Both are directed to improving virus scanning systems. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have applied the disclosure of Bates above to the disclosure of Roberts for the purpose of reducing the time of scanning for a virus, and to ensure that virus status information for URL's in the virus database is kept relatively current (Bates, col. 14 lines 1-5).

Response to Arguments

9. Applicant's arguments with respect to claims 1, 3-7, and 9-13 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's primarily assert that "a factor that the longer the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected the more likely that the file is safe" is not disclosed.

Examiner respectfully disagrees. Bates discloses if the URL was not found to be untrustworthy, control passes to block 98 to determine whether a "good" url threshold time has past-that is, whether an excessive period of time has elapsed since the URL was last virus checked. Figure 3 elements 96-99. Accordingly, a factor that the longer the length of time

(threshold time passed) which the database indicates that the file has been known without malware containing instances of it being detected (no virus in the past)the more likely that the file is safe (checked) .

Conclusion

10. The prior art made of record listed on pto-892 and not relied, if any, upon is considered pertinent to applicant's disclosure.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PHAM whose telephone number is (571)272-3924. The examiner can normally be reached on 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. P./
Examiner, Art Unit 2167

/John R. Cottingham/
Supervisory Patent Examiner, Art Unit 2167